Genera e configura certificati autofirmati per ESA/SMA SAML SSO

Sommario

Introduzione

In questo documento viene descritto come creare certificati autofirmati per la configurazione del provider di servizi SAML (Security Assertion Markup Language).

Prerequisiti

Utilizzare questo documento per generare certificati autofirmati per la configurazione del provider di servizi (SP) SAML (Security Assertion Markup Language) 2.0 Single Sign-On (SSO) su Email Security Appliance (ESA) e Security Management Appliance (SMA).

Requisiti

Metodo 1 (ESA Web UI): Accesso amministrativo ESA nell'interfaccia utente Web e autorizzazione per la gestione dei certificati.

Metodo 2 (comando OpenSSL): OpenSSL installato e disponibile dalla riga di comando.

Windows: Installare OpenSSL.

macOS, Linux o Unix: OpenSSL è in genere disponibile per impostazione predefinita o tramite Gestione pacchetti del sistema operativo.

Componenti usati

Non sono previsti requisiti hardware e software specifici.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento è relativo alle implementazioni di Email Security Appliance (ESA) e Security Management Appliance (SMA) che utilizzano il linguaggio SAML (Security Assertion Markup Language) 2.0 Single Sign-On (SSO). La configurazione di SAML SP richiede certificati SSL (Secure Sockets Layer) per l'installazione del provider di servizi. I certificati possono provenire da strumenti di certificazione interni, da un'Autorità di certificazione (CA) o da un certificato autofirmato.

Problema

In alcune distribuzioni SAML SP per ESA e SMA sono richiesti certificati autofirmati. Questo documento descrive come creare il certificato e la chiave privata e facoltativamente crittografare la chiave privata con una passphrase.

Risoluzione

- In Windows, installare OpenSSL per Windows. Sono disponibili esercitazioni online con istruzioni su come eseguire questa operazione.
- Su Unix, macOS e Linux, OpenSSL è in genere disponibile per impostazione predefinita.
- Utilizzare il metodo di interfaccia utente Web ESA quando ESA già gestisce il certificato e il certificato deve essere esportato per l'utilizzo di SAML SP.
- Utilizzare il metodo di comando OpenSSL quando è necessario creare un certificato e una coppia di chiavi direttamente dalla riga di comando.

Metodo 1: Creazione ed esportazione di un certificato autofirmato nell'interfaccia utente Web ESA

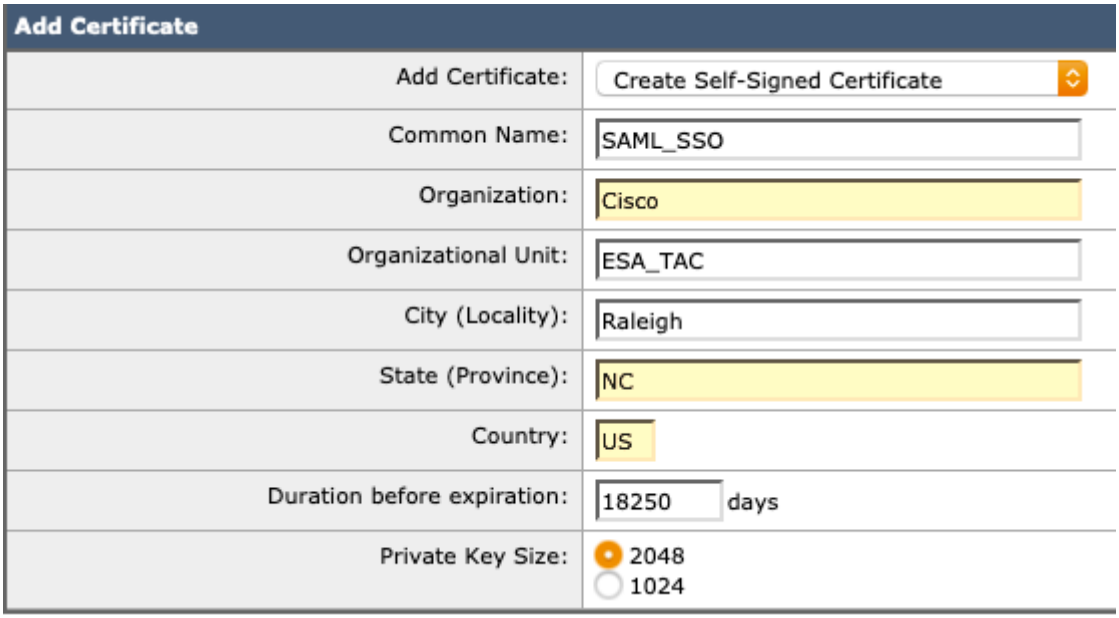
Utilizzare questo metodo quando l'ESA già gestisce il certificato e il certificato deve essere esportato per l'utilizzo da parte dell'SP SAML.

Creare il certificato.

1. Nell'interfaccia utente Web ESA, selezionare Rete > Certificati. Selezionare Aggiungi certificato, quindi Selezionare Crea certificato autofirmato.

2. Inserire i campi del modello: Nome comune, Organizzazione, Unità organizzativa, Città, Stato, Paese e Durata (1-18250 giorni).

3. Impostare la dimensione della chiave privata su 2048.



Completa modello di certificato autofirmato

4. Sottomettere il certificato, esaminare il risultato e selezionare Conferma modifiche.

Certificate Name:	SAML_SSO
Common Name:	SAML_SSO
Organization:	Cisco
Organization Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Signature Issued By:	Common Name (CN): SAML_SSO Organization (O): Cisco Organizational Unit (OU): ESA_TAC Issued On: Sep 20 15:50:27 2019 GMT Expires On: Sep 7 15:50:27 2069 GMT

Visualizza dopo la configurazione

Esportare il certificato.

1. Nell'interfaccia utente Web ESA, selezionare Rete > Certificati > Esporta certificato.

2. Selezionare il certificato da esportare, creare una passphrase, selezionare Esporta e salvare il file in una directory.

Nota: SAML SSO for Administration può importare certificati PKCS#12 (PFX). Se non è richiesta la crittografia a chiave privata, i passaggi di conversione rimanenti sono facoltativi.

Convertire il certificato.

Il certificato esportato è in formato PKCS#12/PFX e richiede la conversione in PEM (Privacy-Enhanced Mail).

Eseguire questo comando OpenSSL per convertire il file PFX nel formato PEM.

<#root>

openssl

```
 pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes
```

<#root>

openssl

```
 pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes
```

Modificare il contenuto e dividere l'output in due file.

1. Il file appena convertito richiede modifiche minori.

2. Aprire due file vuoti in un editor di testo e denominarli <nome>.crt e <nome>.key.

3. Copiare la sezione —BEGIN CERTIFICATE— fino a —END CERTIFICATE— dal file convertito.

4. Incollare il contenuto nel file <nome>.crt e salvarlo.

5. Copiare la sezione —BEGIN PRIVATE KEY— through —END PRIVATE KEY— dal file convertito.

6. Incollare il contenuto nel <name>.key file e salvarlo.

7. È ora possibile caricare il certificato e la chiave nella parte SP SAML della configurazione.

Metodo 2: Utilizzare il comando OpenSSL per creare un certificato autofirmato e una coppia di chiavi

Utilizzare questo metodo quando è necessario creare un certificato e una coppia di chiavi direttamente dalla riga di comando.

Creare la coppia di certificati e chiavi.

Eseguire il comando OpenSSL in un'interfaccia della riga di comando Unix, Linux o macOS. Sostituire domain con il nome richiesto.

<#root>

openssl

 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt

Durante la creazione, vengono visualizzati i prompt per i campi elencati.

Nella directory in cui viene eseguito il comando vengono generati due file: saml_ssl.crt e saml_ssl.key.

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

Crittografare la chiave privata (facoltativo; non richiesto per la configurazione).

Nota: Non riutilizzare le passphrase di esempio. Questa chiave è solo a scopo di esempio.

Questo comando OpenSSL accetta una chiave privata non crittografata (unencrypted.key) e restituisce una chiave crittografata (encrypted.key):

<#root>

openssl

 rsa -des3 -in unencrypted.key -out encrypted.key

<#root>

openssl

```
 rsa -des3 -in saml_sso.key -out saml_secure.key
```

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:


$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

Il certificato e la chiave sono pronti per l'installazione dell'SP SAML SSO o dell'SP SPAM SSO.

Informazioni correlate

Cisco Email Security Appliance - Guide per l'utente

Cisco Content Security Management Appliance - Guide per l'utente

Cisco Web Security - Guide per l'utente

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).